

JavaScript Analysis

- wayback
- gospider
- katana

=> allurls.txt

urls اول حاجه لازم تكون مجمله كل

1- Use Mantra => for api keys

```
Windows PowerShell
root@kali:~/bugbounty/etsy# cat js.txt | mantra

  MANTRA

[Coded by MrEmpy]
[Version 2.1]
[+] https://cdn.dashjs.org/latest/dash.all.min.js [ACK_SELECTION_MODE_HIGHEST_SELECTI]
[+] https://cdn.dashjs.org/latest/dash.all.min.js [APABILITY_MEDIASOURCE_ERROR_MESSAG]
[+] https://advocacy.etsy.com/wp-content/themes/etsy-advocacy/assets/js/app-script.js?ver=1.1
3 [s3.amazonaws.com/]
[+] https://widgets.q4app.com/widgets/q4.api.1.13.1.min.js [apiKey:a]
```

• الاداه بتشتغل زي كذا

• شكل ال api بيبي مكان ال api كذا apiKey:

• لازم تنزل الملفات عندك الاول علي السيرفر عن طريق curl او wget مع for loop

Use jsluice => for secrets and urls => jsluice urls player.js -2

jsluice secrets player.js

for i in \$(ls);do jsluice secrets \$i;done

```
root@kali:~/bugbounty/etsy/js# for i in `cat js.txt`;do wget $i;done
```

• زي كذا

• لازم تعمل فولدر تحطهم فيه وتبقي فيه

```
for i in $(ls);do jsluice secrets $i;done
```

• لو عايز تعملها ع كلو مره واحده

3- Use nuclei => nuclei-templates/http/exposures/

nuclei -l js.txt -t /root/nuclei-templates/http/exposures/ -mhe 4

- حاول تبعد عن ملفات wp علشان الثغرات بتبقى متصلحه
-

4- analyze the code with js beauty in visual studio code

- بتنزل beautify extention

- ctrl+shift+p عشان تشغله